



<https://creativecommons.org/licenses/by/4.0/>

# DESMITIFICANDO A LA DEEP WEB A TRAVÉS DE UN FUGAZ VIAJE POR LA DARK WEB

## *Demystifying the deep web through a fleeting journey through the dark web*

JOHN ALEXANDER RICO FRANCO<sup>1</sup>

Recibido:14 de mayo de 2020. Aceptado:15 de septiembre de 2020

DOI: <http://dx.doi.org/10.21017/rimci.2021.v8.n15.a89>

### RESUMEN

En el instante en que se refiere a la Deep Web y a las DarkNets, la imaginación de aquel que desconoce su realidad, se dispara hacia un entorno lúgubre de la Internet, con la ambientación de una película de anime CyberPunk de los años noventa; lo cual es natural y lógico frente a lo desconocido, ya que inmediatamente se hace referencia a historias folklóricas y ficticias provenientes de múltiples medios, que en particular para el caso aquí referido, son series de televisión, novelas de misterio, entre otros productos provenientes de la ficción; las cuales tienen mucho de exageración y en contadas ocasiones un poco de realidad, aumentando aun más los mitos referentes a la Deep y Dark Webs, los cuales se toman por realidades al ser sectores del ciberespacio aun inexplorados por la mayoría de sus navegantes habituales.

Y es por esto que el presente artículo busca desmitificar un poco la concepción que se tiene de la Deep Web y de las darkNets, buscando dar luz a un ecosistema en línea muy interesante y peligroso a la vez, en el cual se puede encontrar grandes volúmenes de información útil pero que también permite la gestión libre de servicios de comercio de artículos y servicios por fuera de la ley; y para lograr este objetivo, se ha segmentado el presente escrito en cuatro fases primordiales: una introducción básica de que es el ciberespacio y cuáles son sus sectores, para luego pasar a presentar los fundamentos primordiales para conocer el funcionamiento de la Deep Web y de las darkNets, y ya con estos cimientos poder presentar una sesión de navegación segura por la darkNet TOR a través de un laboratorio de navegación resguardado, visita en la cual se exhibirán algunos de los servicios delictivos más comunes allí albergados, para así cerrar el artículo con una conclusión final sobre la realidad del ciberespacio, de sus zonas desconocidas y los peligros que allí se hospedan.

**Palabras clave.** Ciberespacio; Surface Web; Deep Web; Dark Web; darkNet; Tor; Enrutamiento Cebolla; Nodos de Red; Ciberdelincuencia; Protocolo IP; Virtualización.

### ABSTRACT

At the moment when topics related to the Deep Web and the darkNets are treated, the imagination of the one who doesn't know it's reality, is projected towards a gloomy environment of the Internet, with the setting of a CyberPunk anime film of the nineties; activity that is completely logical and normal, because in search of covering the gaps in knowledge, people refer to folk and fictional stories from multiple sources, in particular, television series, mystery novels, among other products from science fiction; references that have a lot of exaggeration and rarely a bit of reality, which increases the myths concerning the Deep and Dark Webs; this is because most of the people take these fictitious references as realities, because these sectors of cyberspace are still a myth unexplored by the most of their casual navigators.

This is why we seek to demystify the conception of the Deep Web and the darkNets and give clarity to a very interesting and dangerous online ecosystem at the same time, because in this mythical sector of cyberspace you can find large volumes of useful information but also allows the free management of criminal commercial services. To achieve this goal, the present document has been segmented into four primary sectors: the first one is a basic introduction of what is

<sup>1</sup> Ingeniero de Sistemas - Especialista en Seguridad de Redes de la Universidad Católica de Colombia, con más de 10 años de experiencia como consultor independiente en proyectos referentes a temas de seguridad informática, criptografía y realización de pruebas de calidad de software. Catedrático Universitario y Docente Investigador del Grupo de Investigación y Desarrollo para la Innovación Sostenible (GIDIS) de la Corporación Universitaria Republicana. Correo electrónico: [jrico@urepublicana.edu.co](mailto:jrico@urepublicana.edu.co) ORCID: <https://orcid.org/0000-0001-6322-0578>

cyberspace and what are its primary sectors, and then proceed to present the fundamentals to know the deployment of the Deep Web and the darkNets, and with these foundations already go on to present a secure browsing session through the darkNet TOR with the help of a virtualized protected navigation environment, that will help to present some of the most common criminal services of the Dark Web, in order to close this article with a final conclusions about the reality of cyberspace, its unknown areas and the dangers that are hosted there.

**Keywords.** Cyberspace; Surface Web; Deep Web; Dark Web; darkNets; Tor; Onion Routing; Network Nodes; Cybercrime; Internet Protocol; Virtualization.

## I. INTRODUCCIÓN

AL MOMENTO de hablar sobre la Deep Web o de las darkNets, la primera concepción que se nos viene a la mente es un lugar digitalizado inhóspito y sucio, casi salido de un cuento de ciencia ficción con tintes de drama policial; en donde los ciberdelincuentes se citan de manera anónima para planear desde sombras cada uno de sus actos criminales, bajo destellos de luces de neón y en ambiente cargado a aromas de cigarrillo, marihuana, licor y comida chatarra.

Pero pasando a un plano menos etéreo y bajo el objetivo primordial de este artículo, desde ya se debe inferir que los conceptos de la Deep y la Dark Web no son sinónimos como se tiende a pensar, ya que al momento de hablar sobre la Deep Web se hace referencia a un vasto sector en la Internet en el cual se aglomera la gran mayoría de páginas y recursos IP que por múltiples razones no pueden y/o deben ser registrados por los buscadores Web convencionales, haciéndolas así invisibles para los navegantes ordinarios que transitan por las zonas conocidas del ciberespacio; mientras que la Dark Web es un sector de la Deep Web, el cual congrega en darkNets los contenidos más sensibles y de índole criminal que se pueden encontrar en el ciberespacio; pero el acceder a esta zona de la Deep Web puede llegar a ser un proceso algo engorroso, ya que al interactuar en espacios ocultos y por ende inhóspitos de la Internet, se requieren de conocimientos básicos de seguridad informática y de redes de datos, ya que al igual que en otros ámbitos, al momento de saber que nos estamos exponiendo a terceros que pueden llegar a perjudicarnos, se debe actuar con cautela para no pasar a ser una víctima sin llegar salir de la comodidad de nuestros hogares.

Así que con esta primera definición básica de que es la Deep y la Dark Web, ya se puede vislumbrar su importancia en la actualidad en temas referentes a la seguridad informática, ya que ambos

son puntos de referencia únicos para descubrir las tendencias delictivas de los cibercriminales modernos, puesto que al evaluar el entorno de gestión de la Deep Web y al ahondar sobre las novedades delictivas publicadas por criminales digitales en foros y salas de chat ocultas que se encuentran distribuidas a lo largo y ancho de las darkNets, se puede esquematizar cuales son los fundamentos verídicos tras los ataques, amenazas y vulnerabilidades computacionales de moda.

Y ya con estas primeras nociones, se puede especificar que la Deep Web es una zona de tránsito entre la Internet conocida (Surface Web) y la Dark Web, por ende es tan importante el poder diferenciar claramente entre estos dos sectores del ciberespacio, que aunque sean ambos poco conocidos, son muy diferentes entre sí; pero al igual que con la naturaleza humana, se debe reconocer que todo lo desconocido y peligroso es mucho más llamativo para nosotros, desde cualquier punto de vista, ya sea desde el ámbito investigativo de la ingeniería de sistemas, o de profundización en la seguridad informática o de simple formación para los navegantes cotidianos que transitan por la Internet; y es que no es de extrañar esta fascinación estimado lector, ya que por ejemplo, los portales Web y servicios ilícitos ofrecidos en las darkNets son bastante interesantes desde el simple sentido de la investigación hasta el morbo que estas generan y son muy especiales desde su concepción y ciclo de vida en el ciberespacio, ya que por ejemplo: los portales de servicios delictivos de mayor éxito en las darkNets tienen un ciclo de vida muy corto, el cual es aproximadamente de 200 días de actividad, lo cual es una maniobra de seguridad muy particular; ya que aunque no fueran detectados por las autoridades, estos sitios Web migran sus servicios al cumplirse dicho tiempo en la nube, como si fuera una estrategia pre-establecida por los ciberdelincuentes implicados; esta táctica elemental es muy efectiva para resguardar la identidad de dichos criminales, ya que debido al alto contenido punible de sus servicios publicados

en las darkNets, son el principal objetivo de las autoridades correspondientes, por lo cual al cerrar de manera repentina el portal de servicios ilegales, suspenden de raíz cualquier proceso de investigación en su contra, lo cual transforma a grandes y muy productivos sitios de comercio electrónico del mercado negro en simples páginas Web desechables, algo indiscutiblemente inesperado e impráctico en la Internet habitual pero que en el entorno por fuera de la ley es completamente viable, ya que esta zona del ciberespacio se ha convertido en el paraíso de los cibercriminales modernos, en el cual se puede ofrecer de manera libre y anónima un variopinto ramillete de negocios delictivos en línea, los cuales van desde el poder contratar los servicios de un sicario a sueldo hasta la compra de drogas recreativas experimentales y todas sus variantes; eso sin querer pasar por la ámbito del entretenimiento para adultos, que analizándolas de manera detallada, se puede apreciar un poco la decadencia de la mayoría de los seres humanos, que al momento de tener un velo de anonimato en línea y gracias a las transacciones económicas incógnitas en Internet, dejan florecer sus más secretos deseos y perversiones, las cuales han encontrado en la Dark Web un lugar único e irrepetible, en el cual sus fantasías, por más retorcidas que estas sean, pueden ser una realidad bajo un alto precio para todos los implicados, convirtiendo a la Dark Web en el purgatorio natural del cielo en la nube de Internet.

## II. CONTEXTO

Para poder entender la realidad de la Deep y Dark Web, se debe conocer como la Internet moderna se compone en realidad, identificar cada una de sus zonas y como estas se comportan entre sí, para así lograr dar un poco de claridad en un entorno tan desconocido actualmente como lo son las periferias recónditas del ciberespacio, tomando a este como todo el conjunto de infraestructura tecnológica, información digital y servicios basados en el protocolo TCP/IP, para gestionar un medio electrónico de telecomunicaciones basado en red de computo a nivel global.

### 2.1 El ciberespacio y su arquitectura:

Al momento de hablar del ciberespacio, se debe tener muy en cuenta que este se encuentra

fraccionado en múltiples capas, las cuales se segmentan según su facilidad de acceso por parte de los navegantes, gestionando así una arquitectura basada en niveles, donde el nivel superior es la Surface Web o la Internet pública, que es la zona del ciberespacio conocida y a la que tiene acceso todos los navegantes, la cual se basa en la consulta de páginas y servicios a través de hiperenlaces HTML y que estos encuentran indexados en todos los buscadores Web libres que abundan en la Internet, para así facilitar su exposición y consulta a todo el público.

Después de la Surface Web sigue la Deep Web, cuyo concepto se basa en ser el sector en el ciberespacio que contenga todo el contenido registrado en la Internet que por múltiples razones no debe ser indexado en buscadores Web tradicionales, en contraprestación a la Surface Web. Entre los elementos albergados en la Deep Web se destacan las páginas privadas que requieren una combinación de credenciales muy particulares para su acceso, páginas de Captcha para acceder a contenido de terceros, páginas que no se encuentran vinculadas a otras directamente, entre otros recursos resguardados en línea, los cuales casi siempre se encuentran vinculados a entidades financieras, gubernamentales, entre otros entes privados y/o públicos que requieren mantener la privacidad de sus contenidos, ya que son exclusivos para sus usuarios autenticados.

Y dentro de la Deep Web coexiste un sector minorista y casi segregado, el cual es la famosa Dark Web, la cual se compone de algunas sub redes anónimas llamadas darkNets, en las cuales se aglutina la gran mayoría de contenidos digitales de índole delincriminal o que son muy sensibles para ser consultados por cualquier persona, por lo cual sus dueños los publican de manera libre y anónima en una subcapa de la Deep Web que es de "difícil" acceso.

En la Fig. 1, claramente se puede vislumbrar como el ciberespacio actual se encuentra esquematizado, en el cual se ve en su apartado izquierdo a la Surface Web, en la cual se albergan todos los recursos en línea a los cuales se pueden acceder por medio de consultas básicas en los buscadores Web tradicionales de Internet; en el sector derecho se encuentra la Deep Web, la cual se compone de dos capas claramente definidas, la primera que

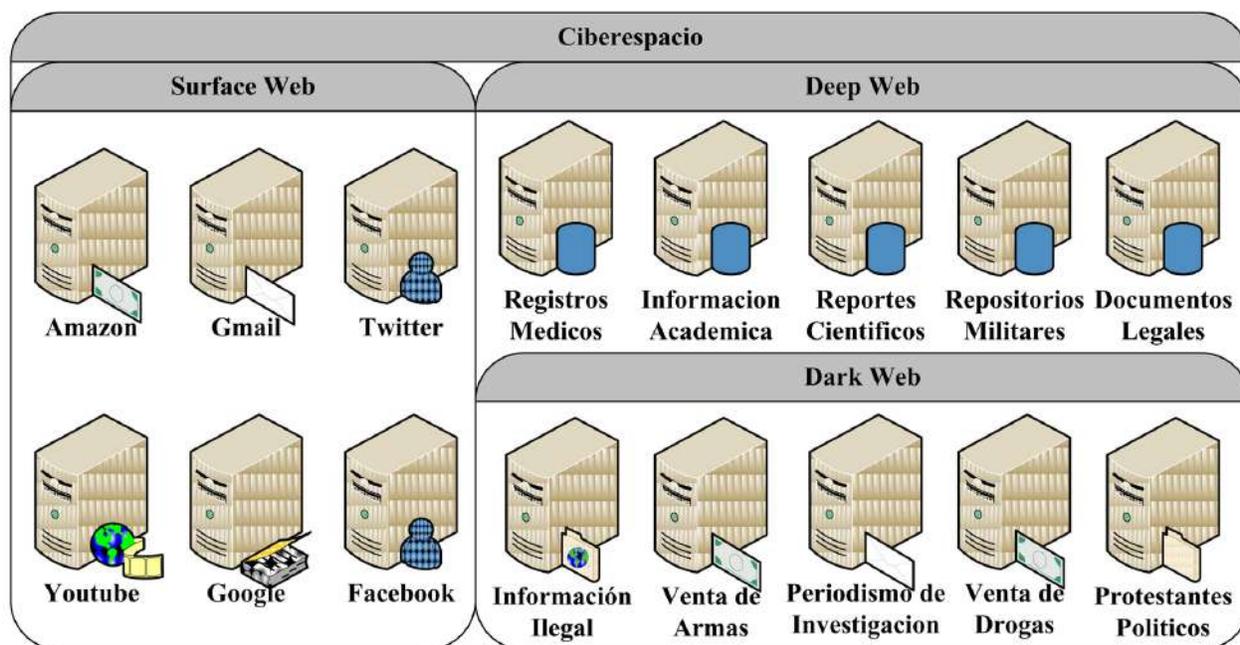


Fig. 1. Arquitectura de Internet por zonas del ciberespacio.

es la básica de la Deep Web, en la cual se encuentran recursos digitales que no deben ser indexados en los buscadores libres, ya que son de uso privativo de sus dueños, como lo son las bases de datos de registros médicos, información académica, reportes científicos, repositorios de datos de índole militar, documentos legales, etc...; en la sub zona de la Deep Web, se puede apreciar el entorno de la Dark Web, en la cual se encuentran por ejemplo aplicaciones y servicios de índole criminal que son ofertados a través de un modelo de comercio electrónico con disposición de mercado negro.

Y ya con esta visión panorámica de que es el ciberespacio y sus distintos componentes, se pasa a presentar a profundidad cada uno de ellos, para así seguir esclareciendo como es el funcionamiento de estos y seguir derrumbando algunos de sus mitos más arraigados.

### 2.1.1 Surface Web

Para poder vislumbrar como es el funcionamiento de la Surface Web, se debe evaluar cómo trabajan los motores de búsqueda típicos de la nube, en los cuales se fundamenta esta red para proporcionar la zona más conocida y amigable del ciberespacio.

Con el nacimiento y evolución de la Internet, se requirió inmediatamente de unos recursos en línea especializados que permitieran la búsqueda en el inmenso ciberespacio de páginas Web según criterios específicos de selección, y es en este instante donde se acuñó el concepto de motor de búsqueda Web, los cuales se analizaron y diseñaron para gestionar exploraciones basadas en palabras específicas en los sitios Web registrados y catalogados en cada motor de consulta, herramientas las cuales se apoyaban en dicha palabra clave de consulta para presentar a través de un entorno de usuario las páginas Web de su catálogo que contuvieran dicha palabra estratégica de sondeo y ordenaban la presentación de resultados según el número de veces que dicha palabra de exploración se repetía en cada una de las páginas de respuesta de la consulta.

Y fue bajo este modelo clásico de ejecución que múltiples motores de búsqueda surgieron en las fases iniciales e incipientes de la Internet; pero esto cambió radicalmente en 1998 con el nacimiento de Google, el cual propuso una revolución en como estas herramientas de consulta en línea debían evolucionar bajo un nuevo paradigma de selección y presentación de los resultados basados en rankings y jerarquía de las páginas consultadas, transfor-

mando radicalmente la manera en cómo funcionan los motores de búsqueda modernos, para evolucionar de simples recursos Web que indexan y presentan resultados, a servicios en la nube de análisis y clasificación de consultas con metodologías de IA. Y ha sido con este nuevo modelo de despliegue de funciones propias de los motores de sondeo Web que se cimentó el concepto de la Surface Web, ya que al poder controlar el cómo y con cuáles recursos se pueden gestionar las consultas, se puede filtrar de manera dinámica a que servicios y páginas pueden ser accedidas por los navegantes básicos y hacer casi invisibles a aquellas que no se encuentren filtradas, almacenadas e indexadas en dichos servicios libres de consulta, logrando por defecto que toda página Web que no se encuentre en dichos servicios de búsqueda, pasen inmediatamente a ser parte de la Deep Web [1].

De manera más específica, la población objetivo de la Surface Web son todos aquellos navegantes casuales que utilizan recursos conocidos de la Internet, que pueden acceder a ellos a través de cualquier navegador que puede consultar a los motores de búsqueda libres que previamente han filtrado y categorizado a los recursos Web catalogados como limpios, por ende los navegantes de este sector de la Internet, no deben tener ningún problema en exponer un poco su identidad e interactuar libremente en las páginas propuestas por dichos motores de búsqueda, ya que un gran porcentaje de estas son fidedignas y de completa confianza, pero no se debe olvidar que algunos atacantes logran engañar a dichos servicios de exploración y logran colar páginas sospechosas o malignas, suplantando a servicios reales y de confianza para tratar de robar información sensible suministrada de manera ingenua por sus dueños [2].

### 2.1.2 Deep Web

La Deep Web aglomera a todos los recursos que se encuentran en la Internet pero que por variadas razones no se les permite estar indexados en los motores de búsqueda públicos y propios de la Surface Web, para así hacerlos prácticamente etéreos para cualquier navegante esporádico del ciberespacio. Por ende, es en esta zona de la Internet en donde se hospedan las páginas dinámicas de consulta privada, las bloqueadas por sus dueños, las de verificación de usuario, los sitios

sin acceso directo o directamente privados; en sí, es en la Deep Web donde se agrupan todos los recursos en línea a los cuales no se desea que cualquier persona pueda conocer su localización a través de una consulta en un motor de búsqueda de índole público [2].

El concepto de Deep Web nace como una respuesta para la poder implementar espacios anónimos y resguardados en una Internet cada vez mas pública y descuidada, la cual se convirtió en una zona desmilitarizada donde se concentra la gran mayoría de la información privada y por ende sensible que fluye por la red de redes, pero también es allí donde se relega a todos los recursos Web sin importancia para los navegantes pero que son de transición para la ejecución asertiva de servicios propios de la computación en la nube y hasta procesos de índole criminal que lógicamente no tienen cabida en la Surface Web.

Y ha sido por este halo de aislamiento propio de la Deep Web, que le ha dado un estatus de peligro y misterio y que es allí donde ocurren todas las actividades criminales que después se verán reflejadas en la Surface Web, concepción que en parte es incorrecta, ya que no es en toda la Deep Web donde se gestionan y efectúan dichas acciones digitales por fuera de la ley, sino que estas son propias de un sector muy específico de la Deep Web, la cual está directamente compuesta por múltiples darkNets para el despliegue de la Dark Web.

### 2.1.3 Dark Web

Gracias a la constante evolución y crecimiento de la Internet, está en los últimos años se ha convertido en el medio de comunicación más importante y masificado existente de la humanidad, en el cual cada vez se genera nueva información y la ya existente se administra de manera automatizada, aparte del hecho de que cada vez son más las personas que pueden consultar e interactuar a través de ella.

Y es por el entorno ágil y en crecimiento del ciberespacio, que se ha hecho una necesidad el intentar supervisar directa o indirectamente el tipo de información que allí circula y como las personas interactúan realmente a través de ella; ya que como todo gran avance de la humanidad, este se

ve condicionado según la manera en como las personas utilizan y aprovechan dichos progresos, ya que ellos por si solos no son ni buenos ni malos, pero estos mutan según como las personas hacen uso de ellos. Entonces al momento de hablar sobre la Dark Web, se debe inferir a un sector segregado de la Deep Web, en el cual se prioriza el anonimato de sus navegantes sin importar las actividades que estos estén gestionando en ella, ya que aparte de que su contenido no está indexado en los motores de búsqueda propios de la Surface Web, como herencia directa de la Deep Web, en la Dark Web se despliega un entorno de cifrado y de enrutamiento de conexiones robusto y complejo, con el único fin de garantizar el anonimato de sus navegantes y que toda la información que estos comparten sea completamente confidencial para cualquier tercero que intente interceptar dicho flujo de información, sin importar la naturaleza de ese tercero en cuestión, así que no importa si este es nativo de la Dark Web, como lo pueden ser los ciberdelincuentes o de índole especial, como lo pueden ser representantes de entidades gubernamentales, de fuerzas de la ley, etc... [3].

En referencia a la funcionalidad de la Dark Web, estas son múltiples, las cuales van desde ser el medio de implementación de actividades delictivas hasta de protección para personas que requieren un entorno seguro de comunicación que no permita la revelación de su identidad a terceros que desean impedir ejercer su derecho a la libertad de expresión, esas dos caras de las darkNets se pueden evidenciar al momento de evaluar dos escenarios típicos de aprovechamiento de la Dark Net; el primero es el delictivo, en donde se utiliza a esta plataforma para implementar acciones de comercio electrónico en la compra y venta de productos ilícitos de manera anónima por parte de criminales alrededor del mundo, de los que se resaltan las transacciones que involucran drogas alucinógenas o de restricción medica, documentos falsificados y armas; pero también existe otro escenario en el cual sus navegantes requieren de una capa de anonimato al momento de comunicarse y expresarse en cualquier red basada en el protocolo IP, como por ejemplo los informantes criminales o disidentes políticos, los cuales su integridad puede verse fuertemente amenazada si llegan a ser descubiertos por las personas de las cuales se está delatando directamente en sus comunicaciones o que

buscan un refugio digital para expresar sus opiniones de manera libre y sin miedo a la censura, ante opresiones gubernamentales o militares de sus respectivos países. Así que no se debe satanizar inmediatamente a la Deep y Dark Web, ya que allí no solamente ocurren actividades ilegales, sino que un muchas ocasiones es el único punto de comunicación para personas que se encuentran en situaciones desesperadas y que requieren que su situación o la de sus seres cercanos sea conocida sin censura y con toda la crudeza que esta requiera [2].

Bajo el apartado de uso delincencial de la Dark Web, las que mayor auge tienen en la actualidad son:

- La compra / venta de armas y de municiones, donde se priorizan aquellos ítems que no se encuentren registrados legalmente o implicados en actividades delictivas previas.
- Compra y venta de drogas, tanto de índole recreativo como legales pero con distribución regulada.
- Foros y páginas informativas de política, hacking y ciberdelincuencia, las cuales buscan adoctrinar a nuevas personas a apoyar ideologías extremistas de índole terrorista o criminal.
- Prestación de servicios de finanzas digitales de índole delictiva, actividades como por ejemplo: venta de tarjetas de crédito y de cuentas de PayPal robadas, lavado de dinero, compra de billetes falsos, entre otros.
- Servicios de Hacking de sombrero negro.
- Venta e intercambio de múltiples tipos de archivos pornográficos, basados en fetiches poco convencionales e ilegales.
- Otros tipos de servicios ilegales, que van desde el poder contratar asesinos y/o maleantes a sueldo hasta la adquisición de documentación falsa sin importar la nacionalidad.

Tal y como se puede apreciar, son múltiples los tipos de servicios delictivos que se encuentran en las darkNets actuales, por lo cual los ciberdelin-

cuentas cada vez son más desconfiados ante sus nuevos clientes, ya que entre ellos pueden encontrar a un representante de la ley con el objetivo de llevarlo a la cárcel; por ende para lograr poder ingresar a dichos servicios ilegales en la Dark Web, el interesado debe pasar por múltiples filtros y pruebas para poder acceder libremente a estos o por lo menos debe ser directamente referenciado por un cliente de confianza, para así poder brindarle al futuro nuevo cliente avalado, un link de acceso protegido en el cual el cibercriminal tiene direccionado ocultamente su portal de mercado negro digital.

Otro aspecto negativo de la Dark Web contemporánea, es que esta no solamente se compone de múltiples portales de compra y venta de productos y servicios ilegales, sino que se ha convertido paulatinamente en un entorno de cultivo para el adoctrinamiento de nuevos cibercriminales, ya que allí pueden encontrar de una manera literalmente fácil múltiples tutoriales y asesorías paso a paso para el despliegue efectivo de actividades de hacking de sombrero negro; logrando así un entorno delictivo algo más complejo al previamente vislumbrado, ya que estos incipientes delincuentes en múltiples ocasiones llegan a estas instancias gracias a su curiosidad o por simple irresponsabilidad, pero en muy contadas oportunidades logran evaluar a cabalidad las consecuencias de sus actos, tanto para ellos como para los terceros victimizados, ya que para la gran mayoría de personas que alcanzan a penetrar a estos niveles de instrucción en la Dark Web, se nutren de un micro modelo social basado en logros delictivos y recompensado con dinero y/o elogios provenientes de sus pares más experimentados [3].

En referencia a los mercados negros de la Dark Web, estos son conocidos comúnmente como criptomercados, los cuales son portales de compra y venta de artículos ilícitos; en estos bazares digitales ilegales, los oferentes publican sus productos y servicios ilegales a través de plataformas similares a Amazon, en las cuales de manera muy fácil pueden presentar las características, precio y rango de distribución de sus productos prohibidos, siempre garantizando el anonimato de todas las partes implicadas, las cuales habitualmente interactúan por medio de avatares y nombres de usuario ficticios, y con un modelo de pago seguro a través de criptodivisas, de las cuales los dueños

de los mercados negros digitales se quedan con una comisión por permitir el desarrollo sin inconvenientes de la transacción, donde la norma es el uso de las Bitcoins, puesto que debido a su naturaleza, su rastreo es casi imposible.

Ya en lo concerniente a actividades de índole sexual que se realizan en la Dark Web, se debe comentar que entre más se profundiza sobre ellas, más tristes y aberrantes son, ya que se ha evidenciado que los delincuentes asociados a dichas actividades monstruosas, han encontrado en ciertos apartados de las darkNets, un punto de encuentro seguro y anónimo, para participar abiertamente con otras personas que tienen sus mismos gustos perversos, con las cuales comparten experiencias, impulsos y hasta “trofeos”; que tristemente realzan su psique inhumana, cruel y criminal, que usualmente no presentarían en su yo análogo o en sus actividades en la Surface Web.

Así que lastimosamente se debe concluir que el manto de anonimato que provee la Dark Web y al ser implementada para la gestión de actividades delictivas, aflora lo peor de cada persona, dejando ver su verdadero ser con cada charla o acción criminal que efectúa a sabiendas de que no está siendo observado y que no tendrá que asumir ninguna culpa o reprimenda por efectuar actividades que de antemano sabe que afectaran directa o indirectamente a terceros, las cuales dejaran huella en sus víctimas de una forma u otra; y es que se puede apreciar que año a año, las diligencias criminales efectuadas en la Dark Web cada vez son más y que a cada rato siguen saliendo nuevos espacios que impulsan a dichos delincuentes a seguir realizando sus fechorías en línea de manera libre y anónima.

Regresando al apartado técnico que soporta a la Dark Web, se debe tener muy presente que este sector de la Deep Web se compone de múltiples darkNets, las cuales son redes privadas que requieren de unos elementos tecnológicos específicos para su acceso y navegación; las darkNets más conocidas son Tor [4] e I2P [5], pero debido a su amplia adopción en entornos prácticos e investigativos, se pasa a profundizar sobre la darkNet Tor.

#### 2.1.3.1 Tor (The Onion Router):

Tor es una red centralizada bajo el protocolo IP, la cual se fundamenta en el uso de nodos

privados para la gestión de la comunicación entre emisores y receptores, por ende el flujo de información entre puntos se gestiona a través de rutas predefinidas de nodos interconectados entre sí.

Tor implementa casi a totalidad la idea clásica de una red de datos centralizada, la cual se basa en la comunicación entre un emisor con un receptor a través del protocolo IP, por medio de nodos identificables para la gestión de rutas o circuitos predefinidos, los cuales son articulados para el intercambio digital de datos. Pero Tor al ser tan ampliamente adoptado a nivel mundial, se compone de múltiples nodos que se encuentran distribuidos en todo el planeta, los cuales para su correcto funcionamiento deben ser administrados a través de listados actualizados de dichos puntos de red privados; hecho que hace fácil su detección al momento de realizar un peritaje del intercambio de paquetes IP entre las partes implicadas en el proceso de comunicación digital, lo cual a primera vista da la percepción de fragilidad, la cual contrasta con el concepto de la Dark Web, por ende para lograr el halo de anonimato por el cual es famosa la darkNet Tor, esta se basa en el concepto de resguardo por capas para enmascarar los nodos de origen y destino al momento de gestionar el proceso de intercambio de datos entre ellos; esta metodología de ocultación es llamada técnicamente como Onion Routing, por la cual todas las direcciones de acceso a recursos en la Dark Web vía Tor son .onion y también esta técnica le asigna su nombre de referencia, Tor = The Onion Router [4] [6].

Entonces se resalta que Tor es una red altamente flexible, ya que de manera transparente se pueden consultar paginas y servicios propios de la Surface Web, como de la Deep y Dark Web, en si a través de Tor indistintamente se pueden hacer consultas tanto de tipología HTTP, HTTPS o .onion.

La metodología de envoltura para el aseguramiento del anonimato a través de Onion Routing, se basa en el uso de múltiples nodos de red distribuidos a nivel mundial y que se encuentran interconectados para gestionar rutas virtuales de comunicación, de los cuales se clasifican según la naturaleza de su trabajo en: nodos de entrada, de paso y de salida, los cuales se especificarán más adelante [7].

Estos nodos privados son aportados por voluntarios anónimos de The Tor Project, la cual es una iniciativa sin ánimo de lucro la cual regulariza e impulsa todo el progreso y manutención de la red Tor, y que desde el año 2002 desarrollo el Browser Tor de manera independiente, el cual es un navegador libre para acceder a dicha red oculta incrustada en la Deep Web [4].

Y ha sido gracias a este impulso dado por The Tor Project y a sus miles de voluntarios dispersos en el mundo, que ha hecho de esta red el bastión del anonimato en la Internet y por ende uno de los pilares de la Dark Web, ya que a mayor cantidad de nodos Tor, mayor es su nivel de resguardo del anonimato de sus navegantes, ya que a más puntos de conexión mas capas de resguardo se gestionan en el proceso de traspaso de datos digitales; y también cabe resaltar que entre más nodos Tor existan, mayor será la velocidad de comunicación en dicha darkNet, ya que así se pueden gestionar mas circuitos y se deja de sobrecargar los ya existentes.

Así que al ser Tor una red centralizada fortificada por múltiples nodos anónimos voluntarios, naturalmente se aumenta la dificultad en el proceso de detección de los circuitos de comunicación propios de dicha darkNet, o de analizar el trafico IP a través de actividades de sniffing propias de los peritos en seguridad informática o de los ciberdelincuentes, logrando así que aunque los nodos Tor lleguen a ser identificados debido a su esquematización centralizada, el proceso de aseguramiento del anonimato de sus navegantes sea robusto; ya que al lograr identificar alguno de los nodos, es muy complejo desenmarañar la capa que identifica al siguiente nodo de paso y así sucesivamente.

Regresando a las bases de la red Tor, tal como se había estipulado anteriormente, esta red de transmisión de datos digitales cumple hasta cierto nivel la idea tradicional de una red IP centralizada, la cual se fundamenta en la comunicación por medio de puntos de red o nodos reconocibles para el despliegue de circuitos virtuales de intercambio de datos, por ende para lograr dicha comunicación asertiva entre nodos, se requiere del uso de autoridades de directorio, los cuales son listas especializadas para empadronar y almacenar la dirección de los múltiples puntos de entrada, de paso o de salida pertenecientes a Tor; estas listas de directorio

son las responsables de administrar la red y de direccionar a los navegantes a través del browser Tor, por medio de las rutas virtuales habilitadas y disponibles [7].

Las autoridades de directorio se encuentran almacenadas directamente en el navegador Tor, para así certificar su autenticidad por defecto y evitar la extracción de las direcciones desprotegidas de los múltiples nodos esparcidos en el mundo que estas contienen; para que así garantizar su anonimato y refrendar su independencia entre sí.

#### 2.1.3.1.1 Funcionamiento de la red Tor:

En el diagrama # 2, se puede apreciar el funcionamiento básico de un proceso de comunicación entre dos puntos a través de la darkNet Tor; en dicho esquema se puede evidenciar a un cliente que desea comunicarse anónimamente con un servidor destino a través de la darkNet Tor, por ende desde el dispositivo cliente y por medio del browser Tor, se comunica a un nodo de ingreso, el cual gestiona un circuito seguro en el que el flujo de información entre el emisor y el receptor debe transitar, (circuito de envío / respuesta el cual esta resaltado en color verde en el diagrama); ya cuando se llega de manera anónima al nodo de salida, este gestiona el proceso de escape de los datos de la darkNet hacia la Surface Web si es que la comunicación es libre, pero si es de otra índole, el punto de salida también se encuentra en dicha darkNet [4] [6] [7].

A continuación se presentan de manera detallada cada uno de los componentes de la darkNet Tor:

##### 2.1.3.1.1.1 Paginas Onion:

Las páginas o servicios Onion, solamente pueden ser consultadas por medio de la red Tor, donde el tráfico que admiten es propio del Onion Routing.

Cabe destacar, que de la misma manera por la cual se ha definido la diferencia entre la Deep y la Dark Web, los servicios Onion no son ni buenos ni malos y pueden ser tan variados según su dueño lo disponga, por lo cual las paginas Onion no refieren indiscutiblemente a servicios delictivos o a la dispersión de cepas de malware, solamente es

que estas son paginas exclusivas de la red Tor y que se encuentran alojadas en dicha darkNet que hace parte de la Deep Web, y que lo único que pueden referir a primería vista es que se desea una comunicación anónima y por fuera de la Surface Web.

Otro de los fines implícitos que tienen los recursos Onion, es que son servicios digitalizados ideales de expresión pública en lugares donde la libertad de expresión es casi nula, también sirven para ser un punto de referencia para la divulgación de ideas provenientes de partidos políticos con ideologías distintas pero legales de las de la tiranía en turno, pero lastimosamente se ha visto una marcada desviación de este último punto, ya que en los últimos años se ha evidenciado que son las entidades radicales y en ocasiones terroristas que toman vocería a través de la Dark Web, para expresarse libremente en contra del gobierno en el poder o de alguna de sus instituciones, sin importar si estas actividades son justificadas o apoyadas por el pueblo.

En el apartado tecnológico, las direcciones de los servicios Onion, se diferencian radicalmente de los nombres de dominio basados en la DNS tradicional de la Surface Web, ya que estos últimos se fundamentan en el uso de nombres propios para la identificación del recurso Web a reseñar, seguidos por una extensión del dominio, como por ejemplo .com o .edu; pero en Tor las cosas son algo más complejas, ya que para poder acceder a un recurso cifrado .onion se debe recurrir a una dirección inteligible de 16 caracteres alfanuméricos seguidos de la extensión de dominio .onion [8].

##### 2.1.3.1.1.2 Nodos de acceso:

Al momento de ingresar a la darkNet Tor se utiliza como portal de ingreso a un nodo de acceso, el cual se encuentra indicado en el listado de las autoridades de directorio incrustadas en el navegador especializado. Este nodo de entrada es el enlace conocido por el browser para ingresar directamente a Tor y este es el responsable de gestionar todo el flujo de información proveniente del usuario hacia la darkNet por medio de los circuitos virtuales de comunicación protegidos [6].

Entonces, cuando el navegante ingresa a Dark Web por medio del browser Tor, esta herramienta

se comunica directamente con un nodo de acceso, el cual sirve como puerta de enlace para ingresar a algunos nodos intermedios y un nodo de salida hacia el receptor de la comunicación, construyendo así un circuito de red virtual resguardado por el cual fluirá la transmisión anónima entre el usuario y los recursos de la Surface, Deep, o Dark Web que desee consultar a través de Tor.

Este punto de enlace es clave para la seguridad implícita de la red Tor, ya que este nodo es el único en todo el circuito de comunicación virtual que conoce la dirección IP del emisor, puesto que este es el que interactúa directamente con el dispositivo cliente; por ende este elemento había sido uno de los puntos más débiles en la darkNet Tor y por lo cual uno de los más atacados por los ciberdelincuentes, pero eso en la actualidad ha sido resuelto, al convertir a las puertas de enlace de ser simples nodos de paso con funcionalidades adicionales a ser puntos de conexión robustos y exclusivos para dicho fin [9].

Ya de manera más detallada, el funcionamiento de los nodos de acceso inicia en el momento en el que usuario solicita su ingreso a la darkNet Tor a través del browser especializado, la herramienta selecciona por medio de su lista de las autoridades de directorio, los nodos de enlace a los que tiene acceso inmediato, entre los cuales elige aquel que este menos congestionado; así que una vez se ha elegido el punto de acceso, se gestiona el circuito de red virtual anónimo, por el cual el cliente va a navegar por Tor.

A diferencia de lo que se presupone, el nodo de acceso no cambia con cada reinicio de conexión, ya que al ser nodos especiales y resguardados dentro de la red Tor, se estipula que estos tengan un ciclo de vida útil de entre 30 a 60 días, según lo ha estipulado The Tor Project; esto con el propósito de controlar activamente el uso de dichos nodos exclusivos de entrada y gestionar en ellos metodologías propias para evitar que sean sobrecargados por peticiones de acceso o ser subutilizados por desconocimiento de su existencia. Otro aspecto por el cual estos nodos de acceso tienen un ciclo de vida tan extenso, según los parámetros de las darkNets, es porque si fueran inconsistentes y de corta vida, los ciberdelincuentes o cualquier persona interesada, podrían suplantarlas fácilmente aprovechándose de la implementación de nodos

de ingreso desechables para establecer supuestos puntos de acceso piratas y maliciosos, que suplanten al original eliminado cándidamente por The Tor Project [4].

#### 2.1.3.1.1.3 Nodos intermedios o de paso:

Un circuito para la transmisión de datos en la darkNet Tor se compone de un nodo de acceso, el cual es el primer punto de gestión del tramo de red virtual anónimo, y de un nodo de salida, que como su nombre lo indica es el punto de red final de dicho circuito, por ende todos los nodos de tránsito, son los requeridos para llegar desde el nodo de ingreso al de salida.

La gran evolución que ha tendido la red Tor en los últimos años se ha nutrido por la gran cantidad de usuarios voluntarios de The Tor Project, quienes gestionan sus propios nodos de paso alrededor del planeta; los cuales se encuentran conectados digitalmente entre si y están dispuestos para la gestión de los circuitos de red virtuales de navegación resguardada vía Tor. Estos nodos intermedios siempre deben estar en constante escrutinio y certificación, para evitar la filtración de nodos falsos y por ende maliciosos controlados por ciberdelincuentes o cualquier ente externo que desee penetrar a esta darkNet [4] [6]. Fig. 2.

Los circuitos de transmisión de la red Tor siempre han sido compuestos por lo menos de tres nodos de paso, para así lograr garantizar un nivel óptimo de anonimato; pero en la actualidad y según parámetros de The Tor Project, estas rutas virtuales se componen de al menos seis nodos de tránsito para la consulta de servicios .onion, gestionando así un canal de conexión mucho más robusto a nivel de seguridad pero algo más lento, ya que al no ser una comunicación directa y con varios repetidores intermedios, los tiempos de la transferencia de datos tendrán desfases de tiempo naturales [4].

Y hablando sobre la seguridad de estos nodos de tránsito, el nivel de confidencialidad entre estos es impuesto por la metodología de cifrado en capas Onion Routing, la cual garantiza que cada punto de recorrido conozca únicamente de que nodo anterior proviene el paquete de datos en tránsito y la dirección del siguiente nodo a quien debe hacer llegar el paquete de datos en circula-

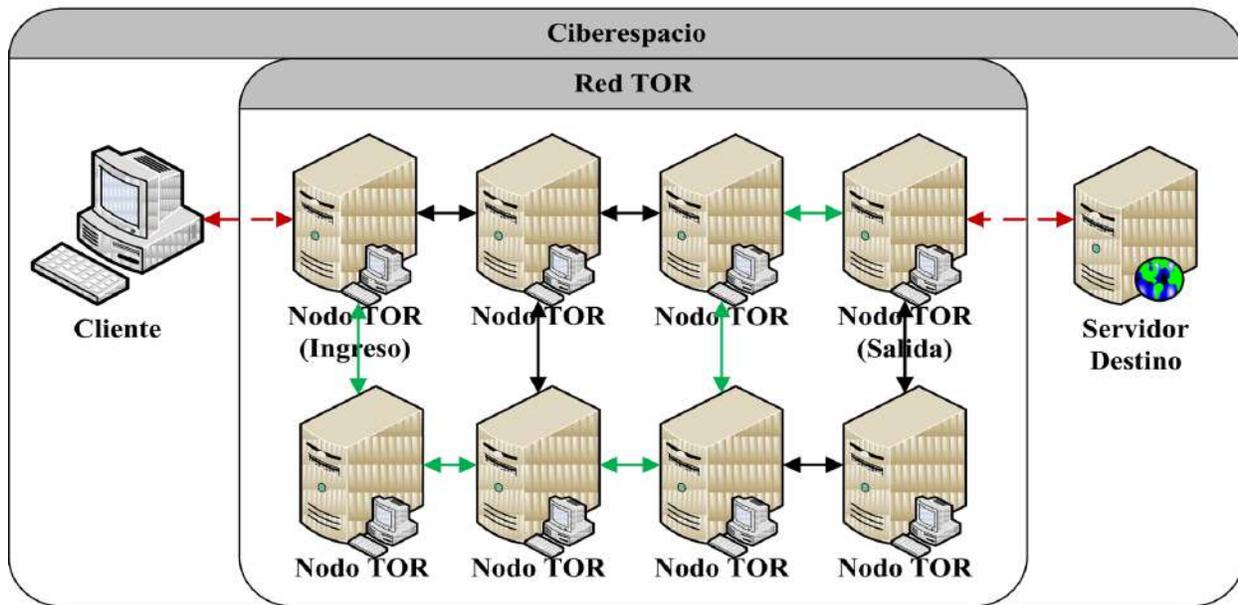


Fig. 2. Esquema básico de funcionamiento de la darkNet Tor.

ción; logrando así que solamente los puntos críticos de entrada y salida conozcan en totalidad el circuito de red virtual y que a medida que se utilicen mas nodos de tránsito, más compleja es la relación entre el cliente y el servidor de la comunicación en ejecución, lo que evita revelar fácilmente la identidad de alguno de los actores involucrados [7] [9].

#### 2.1.3.1.1.4 Nodos de salida:

Los puntos de salida, son los únicos nodos dentro de un proceso de transmisión de datos Tor que interactúa directamente con el destinatario, por ende es el único que conoce su dirección IP, lo que los convierte en sectores de la darkNet Tor altamente sensibles y codiciados por los atacantes al momento de querer vulnerar a dicha red perteneciente a la Dark Web; por lo cual para mitigar arremetidas criminales, tienen el mismo tratamiento privilegiado que poseen los nodos de acceso [9].

Un punto a tener muy en cuenta en este tipo de nodos, es que la información que transita entre el punto de salida y el destinatario se encuentra vulnerable, ya que este nodo es el responsable de desenmarañar la protección por capas implementada a través del protocolo Onion Routing; por ende en la actualidad este proceso de transmisión

final se realiza con la implementación de protocolos criptográficos para su resguardo, los cuales son definidos previamente entre el nodo de salida y el receptor de los datos.

Y debido a la naturaleza de las comunicaciones que se gestionan a través de la red Tor, estas compuertas de salida deben ser tratadas e identificadas metodológicamente, ya que si algún crimen es realizado por medio de dicho nodo, el primer punto de investigación por parte de las autoridades será este elemento de salida, convirtiéndolo en el primer sospecho de la agresión inquirida.

#### 2.1.3.1.1.5 Circuitos de comunicación:

Debido a la naturaleza propia de la darkNet Tor, al momento de transmitir información por ella, los datos van a ser empaquetados y cifrados por capas, según la metodología de Onion Routing, la cual de manera genérica cifra la información de cada capa con una llave criptográfica propia de cada uno de los nodos participantes en el circuito de red virtual anónimo; actividad que se desarrollará desde el primer nodo hasta el último, tal y como es la estructura de una cebolla.

Por ende y al igual que su simbolismo con una cebolla, al momento de gestionar una transmisión por medio de la metodología por capas Onion

Routing, desde la puerta de enlace se cifra el mensaje a emitir con las llaves criptográficas de cada uno de los nodos intermedios que componen al circuito virtual a utilizar en la red Tor, gestionando así un cifrado por capas, en el cual el primer manto de seguridad se desarrolla con la llave criptográfica del último nodo del circuito, la siguiente capa de cifrado se gestiona con la clave del antepenúltimo punto de circulación y así sucesivamente hasta que el último manto de encriptación es implementado con la llave criptográfica del primer nodo de paso; para que así cuando el paquete de datos sea distribuido, cada nodo de transición sea el responsable de descifrar el mensaje con su respectiva llave y así consecutivamente hasta que el último punto termine de decodificar el paquete por completo, para que así este llegue al portal de salida de manera completamente legible para el receptor terminal [7].

Por ende la referencia a una cebolla es más que apropiada para entender a cabalidad a esta metodología de encriptación Web, ya que por medio de la superposición de capas de cifrado, se logra asegurar el dato resguardado en el núcleo del paquete de datos onion.

Cada paquete de datos de tipo Onion, es de un tamaño fijo de 512 bytes, el cual nunca cambia durante su transmisión, aunque el paquete de datos este codificado o no; entonces para garantizar este tamaño fijo, al momento de ser decodificado por uno de los nodos de paso, el espacio ocupado por el cifrado dentro del paquete de datos es reemplazado por información aleatoria de relleno antes de pasar al siguiente punto intermedio; esta actividad se realiza con el fin de evitar una evaluación de ingeniería inversa por parte de algún actor interesado en revelar el funcionamiento del circuito de red virtual en uso, mediante un trazado contrapuesto según la relación del tamaño del paquete de datos en un punto de la ruta de transmisión y el número de nodos previamente recorridos por este [7] [9].

### III. UN PASEO POR LA ZONA PROHIBIDA DE LA DARKNET TOR

Es en este instante, estimado lector, una vez informado de que es la Deep y la Dark Web y algunas de sus características primordiales desde la

visión de la seguridad informática, cuando se debe estar preguntando ¿Cómo puedo acceder a dichas darkNets? y ¿Cómo son los contenidos delictivos allí hospedados?; y en respuesta para satisfacer su deseo de investigación, a continuación se presenta un laboratorio virtual para la inmersión segura en la darkNet Tor, específicamente en la búsqueda de contenido sensible que allí se hospeda, ya que esta actividad en línea se debe realizar con sumo cuidado y protección, ya que no se debe olvidar que allí es el hábitat natural de los ciberdelincuentes actuales, por ende se sugiere que antes de incursionar por la Dark Web, se debe esquematizar un entorno de navegación apropiado, el cual cuenta con dos niveles de protección, uno a nivel de software bajo la implementación de una máquina virtual con la cual se ingresaría a darkNet y uno de comunicación por medio de una VPN, la cual camufla la identidad Web del dispositivo anfitrión de la máquina virtual de inmersión.

El laboratorio de inmersión implementado para el desarrollo del presente artículo se puede evidenciar en la Fig. 3, el cual se fundamenta en la implementación dentro del equipo de cómputo anfitrión de una máquina virtual en la cual se instala en el navegador Tor, para que así cualquier incidente afecte directamente a este elemento virtualizado aislando por software al real; y para resguardar la identidad de dicho dispositivo anfitrión se implementa una VPN [10], la cual para enmascarar la identidad del equipo del laboratorio, asigna una dirección IP de la ciudad de Los Ángeles en Estados Unidos, implementando así una capa extra de anonimato, ya que al momento de consultar recursos hospedados en darkNets de índole delictivo, no se sabe qué medidas de contingencia o de ataque estas ejecutan hacia el navegante.

Ya en el sector de la red Tor, se puede evidenciar despliegue de un circuito virtual de red, el cual se compone de un punto de acceso, de seis nodos de paso y un portal de salida, los cuales para la implementación del laboratorio ejecutado para la realización del presente artículo, en su mayoría se encuentran registrados en Belice, Finlandia, Bulgaria y Alemania.

Antes de iniciar con la inmersión en el sector delictivo presente en la darkNet Tor, es requerido especificar que:

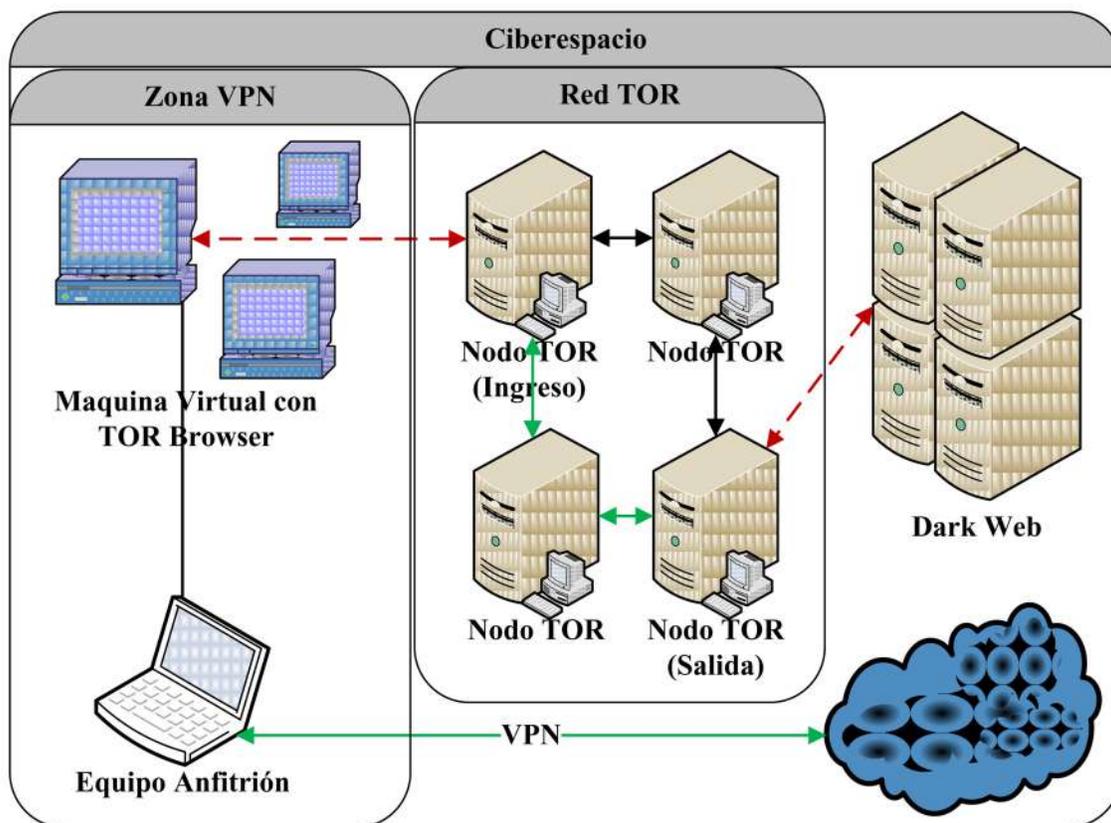


Fig. 3. Arquitectura del laboratorio de inmersión.

- Debido a la magnitud y resguardo de las darkNets y a la sensibilidad de ciertos contenidos, es imposible el poder abarcar a todos los bienes y servicios de índole delictivo que son ofrecidos en ellas, por ende se busca presentar escenarios reales basados en las categorías principales de actividades ciberdelictivas que se llevan a cabo hoy por hoy en Tor.
- No se puede garantizar a un 100% la veracidad de los productos y/o servicios catalogados por fuera de la ley presentados a continuación, esto debido a que es muy habitual que se evidencien páginas que se enfocan a estafar a navegantes primerizos que desean experimentar este lado oscuro del ciberespacio, y son múltiples los sitios de engaño que se hospedan en la Dark Web, ya que estas estafas provienen de múltiples entes, donde se resaltan a dos: el primero es todo el universo de ciberdelictivos que buscan ganar Bitcoins fácilmente al embaucar

navegantes maliciosos sin mucha experiencia en el ámbito ciberdelictivo, y el segundo actor de interés en este escenario son las entidades gubernamentales o fuerzas de la ley que crean portales llamativos con temática criminal, en búsqueda de identificar o directamente cazar a posibles delincuentes en potencia. Pero si se da fe de que todos los ejemplos que posteriormente serán exhibidos, se encuentran publicados en la darkNet Tor y que son considerados por algunos bandos criminales como verídicos.

- Debido a la naturaleza delictiva de los recursos Web que a continuación se exhibirán, no se expondrán sus direcciones de acceso .onion, por más que obvias razones.

Para esquematizar el viaje por la zona roja de Tor, se van a tomar algunos puntos recurrentes basados en servicios criminales presentes actualmente en el lado oscuro de dicha darkNet, los cuales servirán como escalas de trayecto:

1. Venta de documentos de identificación falsos.
2. Comercialización de tarjetas de crédito robadas y de dinero falsificado.
3. Actividades delictivas financieras relacionadas con criptodivisas y lavado de dinero.
4. Compra y venta de drogas y otros elementos ilícitos.

### 3.1 Venta de documentos de identificación falsos:

Todo documento de identificación falsificado, sea nacional o internacional, es una herramienta criminal bastante poderosa en manos de un delincuente, ya que aparte de poder ingresar a países de manera ilegal, también permiten el diligenciamiento de servicios legales que pueden ser utilizados de manera delictiva sin consecuencias reales para el solicitante, ya que al momento de tomar acciones legales sobre el dueño del servicio utilizado de manera maliciosa puede que este sea inexistente o peor aún, se culpará a un tercero inocente mediante la suplantación de su identidad por parte de un bandido.

En las darkNets, son múltiples los sitios que ofrecen la venta de dichos documentos de identificación falsificados, los cuales los más frecuentemente ofertados son pasaportes, licencias de conducción, tarjetas de identificación, visas, entre otros documentos legales, supuestamente indetectables, sin importar el país de expedición o la naturaleza del documento.

Ya en el apartado de venta de pasaportes falsos, existe un sinnúmero de portales “especializados” en la venta de dichos elementos de identificación internacional; en una página básica de dichos productos falsificados, se ofrecen pasaportes, tarjetas de identificación y licencias de conducción, como se puede apreciar en el ejemplo exhibido en la Fig. 4:

En el ejemplo expuesto en la Fig. 4, se puede apreciar que dicho portal de venta ofrecen una gran variedad de documentos de identificación supuestamente originales de Australia, Bélgica, Brasil, Canadá, Finlandia, Francia, Alemania, Irlanda, Italia, Malasia, Holanda, Noruega, España, Suecia, Sui-

za, Inglaterra y Estados Unidos; junto con certificados de IELTS, TOEFL y ESOL.

En las Fig. 5 y Fig. 6, se presentan algunos ejemplos “reales” de los productos ofertados en el portal presentado en la Fig. 4:

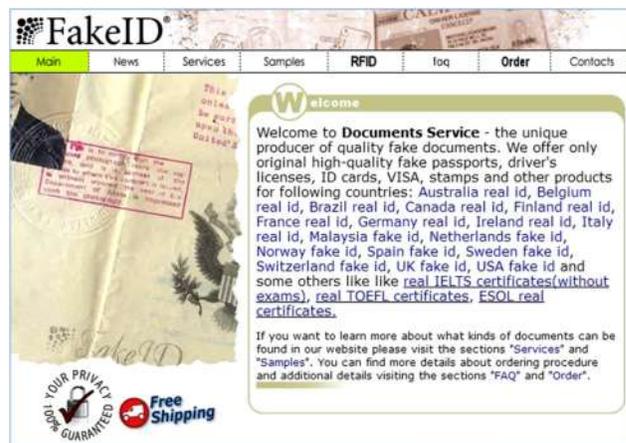


Fig. 4. Portal de venta de documentos de identificación falsos.



Fig. 5. Publicación de venta de pasaportes falsificados.

Pero no todas las páginas referentes a la venta de documentación falsificada son tan diversificadas, por ejemplo en el transcurso de la navegación en la darkNet Tor, se encontraron dos páginas especializadas exclusivamente en la comercialización de licencias de conducción falsas, las cuales se pueden apreciar en las Fig. 7 y Fig. 8:



Fig. 6. Oferta de documentos de identificación falsos.



Fig. 8. Comercialización de licencias de conducción europeas falsas.

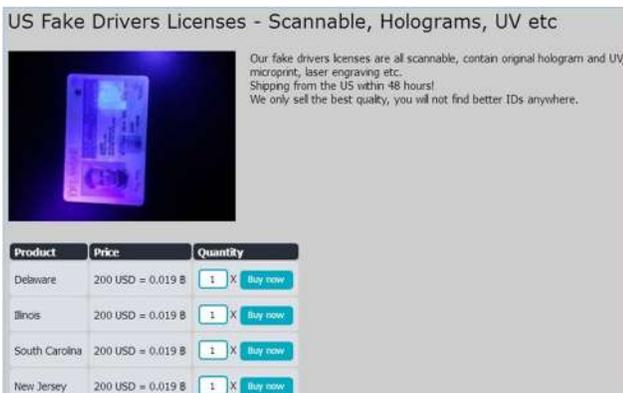


Fig. 7. Venta de licencias de conducción estadounidenses falsas.



Fig. 9. Publicación de oferta de títulos universitarios y de prescripciones medicas falsas.



Fig. 10. Oferta de servicios ilegales para la obtención de la ciudadanía estadounidense.

Pero no solo se encuentran documentos referentes a identificación falsos en la Dark Web, también se encuentran paginas especializadas para la venta de títulos universitarios inexistentes y para obtener la ciudadanía americana por un muy alto precio, en el año 2019, la tarifa estándar de dicho servicio es de \$ 3.000 dólares. Fig. 9 y 10.

Los precios de dichos documentos falsificados varían, según su nacionalidad, naturaleza, el país desde donde es ofrecido, del vendedor que lo ofrece, etc...; ya que es distinto un pasaporte afgano ofrecido por un vendedor desconocido que radica en las Islas Caimanes que un soporte de ciudadanía estadounidense ofertado por una asociación

criminal “reconocida” a través de un portal de compraventa “seguro” y oculto dentro de la Dark Web, al cual solamente se puede acceder a través de invitaciones provenientes de clientes certificados y con cierto nivel de antigüedad dentro de la comunidad ciberdelictiva.

### 3.2 Comercialización de tarjetas de crédito robadas y de dinero falso:

Es habitual encontrar en la Dark Web, páginas “especializadas” en la venta de dinero falso, el cual obviamente aseguran que es idéntico al real; del cual ofrecen de múltiples divisas y denominaciones; pero es de resaltar que las monedas más falsificadas son el Euro, el Dólar Estadounidense y la Libra Esterlina. Fig. 11, 12 y 13.



Our notes are produced of cotton based paper. They pass the pen test without problems. UVi is incorporated, so they pass the UV test as well. They have all necessary security features to be spent at most retailers. Free shipping in the US.

Product	Price	Quantity
25 x 50 USD	325 USD = 0.03109 \$	1 x Buy now
50 x 50 USD	500 USD = 0.04783 \$	1 x Buy now
100 x 50 USD	900 USD = 0.08610 \$	1 x Buy now

Fig. 11. Comercialización de dólares falsos.



Our notes are produced of cotton based paper. They pass the pen test without problems. UVi is incorporated, so they pass the UV test as well. They have all necessary security features to be spent at most retailers. FREE EXPRESS SHIPPING! We are shipping from France!

Update: lowered prices for old 50 EUR series, new series will be in stock later. Notes can still be used in every shop in Europe, only avoid banks as usual.

Product	Price	Quantity
25 x 50 Euro Bills	275 EUR = 0.02819 \$	1 x Buy now
60 x 50 Euro Bills	490 EUR = 0.05023 \$	1 x Buy now
120 x 50 Euro Bills	850 EUR = 0.08714 \$	1 x Buy now

Fig. 12. Venta de euros falsificados.



Money the Easy & Safe Way!

Stay away from counterfeit methods that will send you to jail.

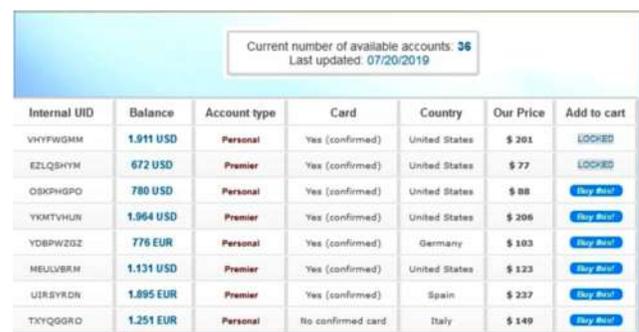
- NO PayPal Digital Trail
- NO Bank Transfer Fraud
- NO ATM Camera Recording
- NO Distracting the Cashier

Proven to be 100% safe  
Happy Customers over 3,000 + Reviews  
Deposit it in vending machines, bank accounts or ATM's with complete safety.

Fig. 13. Oferta de libras esterlinas falsas.

Es habitual en el entorno de la Dark Web, encontrar portales especializados en la venta de cuentas de servicios bancarios como PayPal, tarjetas de crédito y débito, entre otros; de los cuales ofrecen múltiples variedades de cuentas, supuestamente reales, las cuales varían en precio según el balance que tienen en crédito.

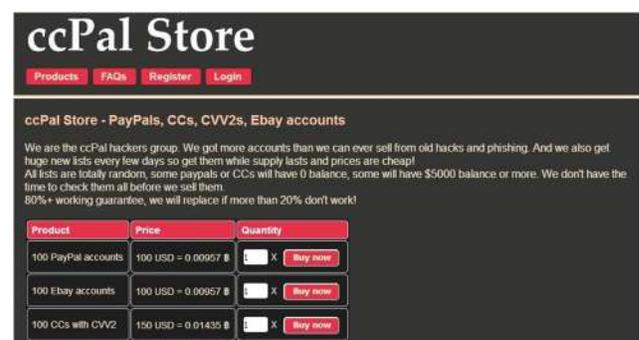
En referencia a la oferta ilícita de cuentas de servicios alternativos financieros, en la Dark Web existen dos modelos de comercio referentes, una en donde se pueden conseguir individualmente, identificando el saldo disponible y otra donde se venden paquetes compuestos de un número determinado de cuentas, en las cuales el vendedor no garantiza su vigencia y saldo disponible. Estos dos ejemplos se pueden apreciar en las Fig. 14 y Fig. 15.



Current number of available accounts: 36  
Last updated: 07/20/2019

Internal UID	Balance	Account type	Card	Country	Our Price	Add to cart
VHYFWGMM	1,911 USD	Personal	Yes (confirmed)	United States	\$ 201	LOCKED
EZLQSHYM	672 USD	Premier	Yes (confirmed)	United States	\$ 77	LOCKED
ODKPHGPO	780 USD	Personal	Yes (confirmed)	United States	\$ 88	Buy Now
YKMTVHUR	1,964 USD	Premier	Yes (confirmed)	United States	\$ 206	Buy Now
YDHPWZJZ	776 EUR	Personal	Yes (confirmed)	Germany	\$ 103	Buy Now
MEULVBRM	1,131 USD	Premier	Yes (confirmed)	United States	\$ 123	Buy Now
UIRSYRDN	1,895 EUR	Premier	Yes (confirmed)	Spain	\$ 227	Buy Now
TKYQGGRO	1,251 EUR	Personal	No confirmed card	Italy	\$ 149	Buy Now

Fig. 14. Página de venta fraudulenta de cuentas de PayPal individuales.



ccPal Store - PayPals, CCs, CVV2s, Ebay accounts

We are the ccPal hackers group. We got more accounts than we can ever sell from old hacks and phishing. And we also get huge new lists every few days so get them while supply lasts and prices are cheap! All lists are totally random, some paypals or CCs will have 0 balance, some will have \$5000 balance or more. We don't have the time to check them all before we sell them. 80%+ working guarantee, we will replace if more than 20% don't work!

Product	Price	Quantity
100 PayPal accounts	100 USD = 0.00957 \$	1 x Buy now
100 Ebay accounts	100 USD = 0.00957 \$	1 x Buy now
100 CCs with CVV2	150 USD = 0.01435 \$	1 x Buy now

Fig. 15. Comercialización de paquetes de cuentas de Ebay, PayPal y tarjetas de crédito.

Y de en búsqueda de diversificar sus actividades delincuenciales referentes a la clonación de tarjetas de crédito, los cibercriminales ahora las ofrecen en formato físico, en las cuales se falsifica el plástico y la banda magnética para hacerlas pasar por originales; las cuales son desarrolladas

según las especificaciones del comprador, sin importar la entidad bancaria a suplantar, el nombre y número de registro de la tarjeta crédito.

De las actividades por fuera de la ley presentadas en este apartado, la clonación física de tarjetas de crédito es la que en mas auge tiene actualmente entre la comunidad delictiva digital y es la que más llama la atención a las organizaciones especializadas en asegurar estos activos financieros, ya que su aparición indica la existencia de entidades delictivas profesionales y organizadas, ya que se requiere de software y hardware especializado para la realización de ese tipo falsificaciones. Fig. 16 y 17.

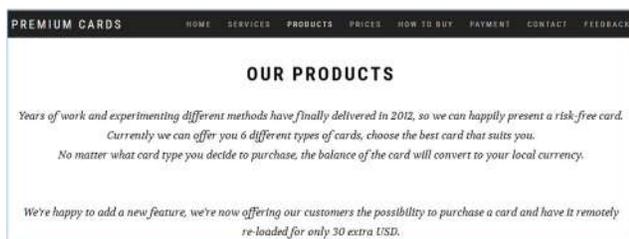


Fig. 16. Pagina de presentación de servicios de clonación física de tarjetas de crédito.

USD/CAD/AUD		EURO/GBP		AMEX	
FROM \$	130	FROM \$	150	FROM \$	250
1 CARD -	\$130	1 CARD -	\$130	1 CARD -	\$250
2 CARDS -	\$240	2 CARDS -	\$270	2 CARDS -	\$450
3 CARDS -	\$300	3 CARDS -	\$360	3 CARDS -	\$600
5 CARDS -	\$450	5 CARDS -	\$450	5 CARDS -	\$1100
7 CARDS -	\$570	7 CARDS -	\$600	7 CARDS -	\$1400
10 CARDS -	\$800	10 CARDS -	\$780	10 CARDS -	\$1900

Fig. 17. Tabla de tarifas de servicios de clonación física de tarjetas de crédito.

### 3.3. Actividades delictivas financieras relacionadas con criptomonedas y lavado de dinero:

Desde un principio, el bitcoin fue declarada la divisa por defecto de la Dark Web, debido a su independencia a un país o región en particular y a su estructura de protección criptográfica en las transacciones financieras digitales basadas en ella, por ende gestiona un entorno de comercio electrónico con un alto nivel de anonimato y resguardo, sin importar si estas actividades son de índole legal o

no; así que era solo cuestión de tiempo para que los cibercriminales esquematizaran un modelo económico ilegal bajo esta criptomoneda, ya que es relativamente fácil el poder formalizar actividades financieras por fuera de la ley de manera incógnita y transparente, de manera casi similar a las implementadas en la Surface Web, pero con un nivel de seguridad nativo mucho más robusto e independiente, basado en los privilegios y metodologías aportadas por la criptomoneda Bitcoin, las cuales serán completamente anónimas, siempre y cuando el comprador no vincule su billetera virtual real al momento de desarrollar una compra ilegal en alguna darkNet, ya que en ese caso, la transacción si será completamente identificable y por ende rastreable en una investigación policial o por algún ciberdelincuente que desee robar dicha billetera o en últimas instancias para chantajear al comprador.

Ya en referencia a las actividades financieras ilegales ofertadas en las zonas rojas de Tor, la más común es el de lavado de criptomonedas utilizadas en actividades delictivas previas, esta tarea se basa en la "mezcla" de transacciones legales realizadas con dichos recursos financieros digitales de dudosa procedencia. Este servicio siempre es ejecutado por un tercero que tenga un pasado judicial transparente y que realice movimientos económicos basados en dicha divisa de manera frecuente; esta actividad inicia cuando se segmenta la totalidad de criptomonedas sombrías en miles de micro transacciones de compra y venta licitas, pasando dicha cantidad de dinero digital de una divisa a otra, para así limpiarla artificialmente por ciclos repetitivos, una vez se han gestado algunos de estos ciclos de lavado, se retorna la cantidad de crédito implicado ya limpio y proveniente de una transacción completamente transparente en la Surface Web, esta técnica de lavado de criptomonedas se conoce en el mercado negro como Mixing.

Son muchas las páginas en la darkNet Tor que ofrecen dicho servicio financiero ilegal de lavado de criptomonedas y cada vez evolucionan para presentar un diseño amigable y muy profesional. Fig. 18, 19 y 20.

Otro modelo económico al margen de la ley que en estos días está en furor en las darkNets, es la compra directa de criptomonedas en dinero en efectivo o por crédito bancario "certificado", a unas



Fig. 18. Portal de servicios de lavado de bitcoins.



Fig. 19. Presentación de los beneficios al utilizar servicios de lavado de bitcoins.

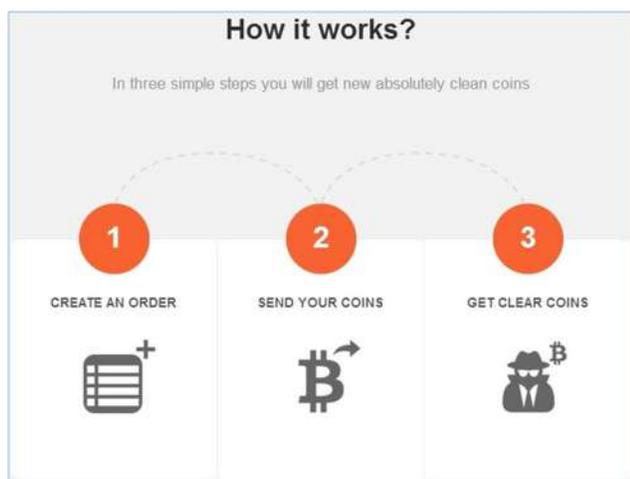


Fig. 20. Esquema de ejecución del lavado de criptomonedas por medio del método de mezcla.

altas tasas de cambio y sin importar el tipo de moneda solicitado por el vendedor; condiciones que son mucho más llamativas y beneficiosas que los servicios ofrecidos por entidades bancarias lícitas en la Surface Web.

El actual auge de esta actividad financiera ambigua radica en evitar directamente actividades de lavado de criptomonedas de dudosa procedencia, en las cuales se debe entregar ciegamente a un tercero desconocido cierta cantidad de dinero

digital y esperar días hasta que este capital regrese a su dueño, en sí, es un salto de fe entre ladrones, el cual muy pocas personas estarían dispuestas a aceptar.

### 3.4 Compra y venta de drogas y otros elementos ilícitos:

El mayor mercado de comercio electrónico ilegal presente actualmente en las darkNets, es el referente a la venta y compra de distintos productos por fuera de la ley, donde los más presentes son las armas y las drogas, tanto las recreacionales como las recetadas con distribución limitada debido a sus efectos colaterales o a su grado de adicción si no se controla su consumo por un médico certificado para dicha actividad.

Este mercado negro ilegal fue la base del reconocimiento de la Dark Web como un medio digital para la adquisición de dichos productos prohibidos, ya que fue en el año 2013 cuando este modelo económico criminal fue exhibido a todo el mundo, cuando el portal de comercio electrónico ilegal más grande hasta el momento fue cerrado, el cual era el infamemente famoso Silk Road, que fue diseñado y desplegado por Ross William Ulbrich, que cuyo pseudónimo en la Dark Web era Dread Pirate Roberts y que gracias a su portal Silk Road cobraba un porcentaje por cada una de las transacciones ilícitas o no que allí se generaban; en 2015 fue condenado por el gobierno de los Estados Unidos por cargos de narcotráfico, lavado de activos, ciberdelincuencia y contrato a sicarios, en la actualidad se encuentra purgando una condena de por vida en Centro Correccional Metropolitano de Nueva York.

Pero estos antecedentes adversos no han frenado a los ciberdelincuentes para seguir en sus actividades mercantiles basadas en la transacción de productos ilegales, y es que paseando por la darkNet se encuentran muchas pequeñas paginas centralizadas en dicha actividad, en donde se encuentran algunas especializadas en drogas sintéticas, alucinógenos naturales y de armas sin registro o que estén previamente implicadas en incidentes delincuenciales. Fig. 21 a 24.

En la actualidad no se ha visto un mercado negro en línea tan prospero como lo llego a ser en su tiempo Silk Road, pero cada vez son más los pequeños portales de comercio electrónico que

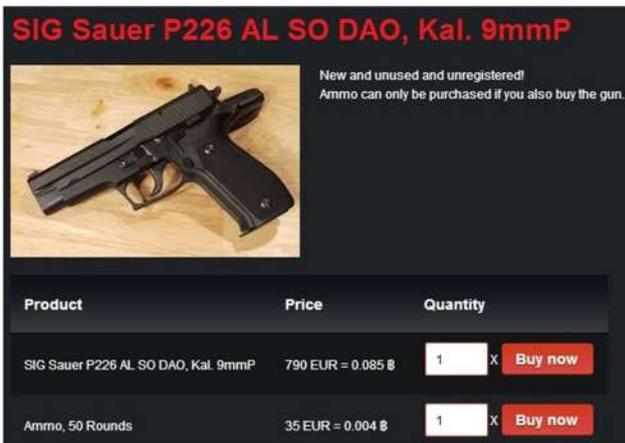


Fig. 21. Comercio de armas y municiones ilegales.



Fig. 22. Ejemplo de una pagina básica para la venta de drogas alucinógenas.



Fig. 23. Oferta de marihuana con fines completamente recreativos.

emulan a grandes empresas legales en este rublo, como lo son Amazon y Ebay, pero que se enfocan en facilitar las transacciones ilícitas que involucran productos y/o servicios ilegales. Fig. 25 a 27.

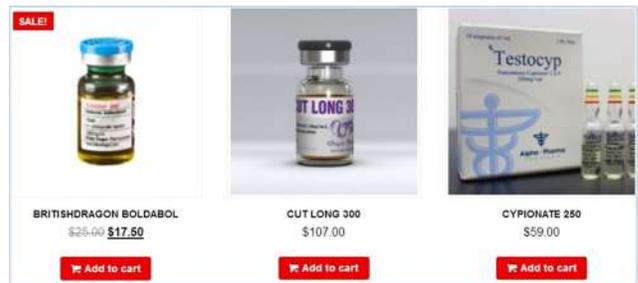


Fig. 24. Venta de medicina altamente controlada.



Fig. 25. Portal de comercio electrónico enfocado a la venta de armas.

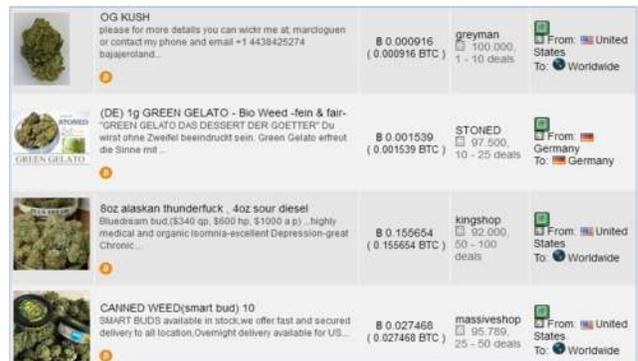


Fig. 26. Portal de comercio electrónico enfocado a la venta de drogas orgánicas.

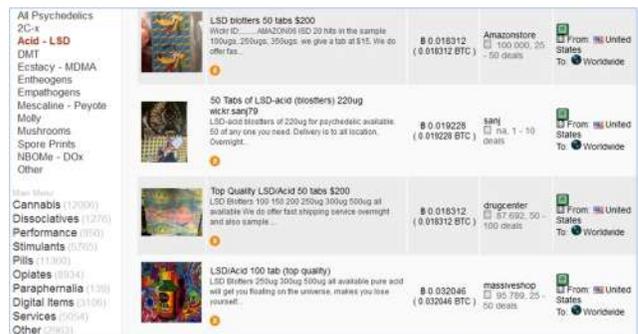


Fig. 27. Portal de comercio electrónico enfocado a la venta de drogas sintéticas.

## IV. CONCLUSIONES

Lamentablemente, el concepto más llamativo de la Dark Net, es como esta afecta la manera en el cómo se concibe la Internet actualmente, ya que desde el apartado técnico, genera una zona altamente segura en un ambiente más que inseguro y volátil; pero lastimosamente como toda tecnología, esta se rige por completo según como sea utilizada, y tristemente la Dark Web es infamante famosa debido a su uso para la realización de actividades criminales en la nube, acciones las cuales no solamente han dado mala fama a la Dark Web sino que han llegado a enlodar a la Deep Web; esto debido a que en muchas ocasiones, los medios de comunicación no especializados utilizan erróneamente a la Deep Web como sinónimo de la Dark Web y viceversa; por ende, una de las finalidades del presente artículo era el reivindicar un poco el nombre de la Deep Web y enfatizar el hecho de que la Dark Web no solamente es un mecanismo exclusivo de los ciberdelincuentes y realzar que esta tiene un potencial más que brillante en el momento en que se utiliza de manera responsable; ya que por ejemplo, es gracias al uso adecuado de las darkNets que se logra conocer la realidad en países con gobernantes con tendencias dictatoriales, que implementan censura de toda la información saliente de sus naciones y que filtran las noticias provenientes del resto del mundo, en búsqueda de que su feudo se mantenga desinformado y sin voz en el planeta.

Y por último, si alguna vez, usted estimado lector, desea visitar la Dark Web con un alto sentido de la aventura, por favor no compre nada ilegal o pague por un servicio prohibido, para así no seguir financiando un modelo económico criminal, en el cual existen múltiples víctimas y que contiene altos riesgos para su seguridad, si no navega por ella sin las debidas consideraciones.

## REFERENCIAS

- [1] P. Abraham. "A look at the history of Google and how it was founded". ZNETLIVE Blog. [Internet]. Disponible en <https://www.znetlive.com/blog/a-look-at-the-history-of-google-and-how-it-was-founded/>. 2018
- [2] M. Bergman. "The Deep Web: Surfacing Hidden Value". *The Journal of Electronic Publishing [JEP]*. [Internet]. Vol. 7 n.º 1. Disponible en <https://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main>. 2001.
- [3] D. Sui, J. Caverlee y D. Rudesill. "The Deep Web and The DarkNet: A look inside the Internet's massive black box". [Internet]. Disponible en [https://www.wilsoncenter.org/sites/default/files/stip\\_dark\\_web.pdf](https://www.wilsoncenter.org/sites/default/files/stip_dark_web.pdf). 2015.
- [4] "Tor Project | Anonymity Online". [Internet]. Disponible en <https://www.torproject.org/>. 2019.
- [5] "I2P Anonymous Network". [Internet]. Disponible en <https://geti2p.net/en/>. 2019.
- [6] L. Henderson, *Tor and the Dark Art of Anonymity*, 1.ª ed., California: CreateSpace Independent Publishing Platform; 2015.
- [7] M. G. Reed, P. F. Syverson y D. M. Goldschlag. "Anonymous Connections and Onion Routing". *IEEE Journal on Selected Areas in Communications*. [Internet]. Vol. 16 n.º 4. Disponible en <https://www.onion-router.net/Publications/JSAC-1998.pdf>. 1998.
- [8] P. Winter, A. Edmundson, L. M. Roberts *et al.* "How do Tor users interact with Onion Services". [Internet]. Disponible en <https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-winter.pdf>. 2018.
- [9] D. McCoy, K. Bauer, D. Grunwald *et al.* "Shining Light in Dark Places: Understanding the Tor Network". *PETS '08 Proceedings of the 8th international symposium on Privacy Enhancing Technologies*. [Internet]. Disponible en [https://homes.cs.washington.edu/~yoshi/papers/Tor/PETS2008\\_37.pdf](https://homes.cs.washington.edu/~yoshi/papers/Tor/PETS2008_37.pdf). 2008.
- [10] "ExpressVPN". [Internet]. Disponible en <https://www.expressvpn.com>. 2019.